

This is a repository copy of *Quantum Circuits for Quantum Channels*.

White Rose Research Online URL for this paper:

<https://eprints.whiterose.ac.uk/116215/>

Version: Accepted Version

Article:

Iten, Raban, Colbeck, Roger Andrew orcid.org/0000-0003-3591-0576 and Christandl, Matthias (2017) Quantum Circuits for Quantum Channels. Physical Review A. 052316. ISSN 1094-1622

<https://doi.org/10.1103/PhysRevA.95.052316>

Reuse

Items deposited in White Rose Research Online are protected by copyright, with all rights reserved unless indicated otherwise. They may be downloaded and/or printed for private study, or other acts as permitted by national copyright laws. The publisher or other rights holders may allow further reproduction and re-use of the full text version. This is indicated by the licence information on the White Rose Research Online record for the item.

Takedown

If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.

Quantum Circuits for Quantum Channels

Raban Iten,^{1,*} Roger Colbeck,^{2,†} and Matthias Christandl^{3,‡}

¹*Institute for Theoretical Physics, ETH Zürich, 8093 Zürich, Switzerland*

²*Department of Mathematics, University of York, YO10 5DD, UK*

³*QMATH, Department of Mathematical Sciences, University of Copenhagen, Universitetsparken 5, 2100 Copenhagen, Denmark*

(Dated: 10th May 2017)

We study the implementation of quantum channels with quantum computers while minimizing the experimental cost, measured in terms of the number of Controlled-NOT (C-NOT) gates required (single-qubit gates are free). We consider three different models. In the first, the Quantum Circuit Model (QCM), we consider sequences of single-qubit and C-NOT gates and allow qubits to be traced out at the end of the gate sequence. In the second (RandomQCM), we also allow external classical randomness. In the third (MeasuredQCM) we also allow measurements followed by operations that are classically controlled on the outcomes. We prove lower bounds on the number of C-NOT gates required and give near-optimal decompositions in almost all cases. Our main result is a MeasuredQCM circuit for any channel from m qubits to n qubits that uses at most one ancilla and has a low C-NOT count. We give explicit examples for small numbers of qubits that provide the lowest known C-NOT counts.

I. INTRODUCTION

Quantum channels, mathematically described by completely positive, trace-preserving maps, play an important role in quantum information theory because they are the most general evolutions quantum systems can undergo. The ability to experimentally perform an arbitrary channel enables the simulation of noisy channels. For example, this is useful to test how a new component (e.g., a receiver) will perform when subjected to noise in a more controlled environment. Moreover, experimental groups can show their command over quantum systems consisting of a small number of qubits by demonstrating the ability to perform arbitrary quantum channels on them (see for example [1] and references therein). Instead of building a different device for the implementation of each quantum channel, it is convenient to decompose arbitrary channels into a sequence of simple-to-perform operations. In this paper we work with a gate set consisting of C-NOT and single-qubit gates, which is universal [2]. However, note that the main ideas of our circuit constructions and lower bounds generalize to arbitrary gate sets. The implementation of a C-NOT gate is usually more prone to errors than the implementation of single-qubit gates. For example, the lowest achieved infidelities are by a factor of more than 10 smaller for single-qubit gates than for two qubit gates [3, 4]. This motivates using the number of C-NOT gates to measure the cost of a quantum circuit.¹

In this work we consider the construction of universal circuit topologies comprising gates from this universal set. A circuit topology [5, 6] corresponds to a set of quantum channels that have a particular structure but in which some gates may be free or have free parameters. Our aim is to find circuit topologies that minimize the C-NOT count but are universal in the sense that any channel from m to n qubits can be obtained by choosing the free parameters appropriately.

We work with three different models. In the first we consider *the quantum circuit model* (QCM), in which we allow a sequence of C-NOT, single-qubit gates and partial trace operations on the qubits and any ancilla. In the second (RandomQCM) we allow the use of classical randomness in addition. In the third (MeasuredQCM), we allow the operations of the QCM as well as measurements and operations that are classically controlled on the measurement outcomes.

A task that is related to the construction of a circuit topology is that of minimizing the C-NOT count for a given quantum channel (on a channel-by-channel basis). Although this appears quite different, we show that it is related in the sense that our lower bounds on the number of C-NOT gates for circuit topologies that are able to generate all quantum channels of Kraus rank K are also lower bounds for almost all (in a mathematical sense) quantum channels of Kraus rank K individually, where the Kraus rank of a channel is defined as the smallest number of Kraus operators required to represent the channel and is equal to the rank of the corresponding Choi state [7].

It is worth emphasizing that there is a (measure zero) set of channels for which our lower bounds do not apply individually, and this set contains experimentally inter-

*Electronic address: itenr@itp.phys.ethz.ch

†Electronic address: roger.colbeck@york.ac.uk

‡Electronic address: christandl@math.ku.dk

¹ Certain experimental architectures only allow nearest neighbour C-NOT gates. Here we assign the same cost to each C-NOT gate regardless of its interaction distance. However, our circuit constructions for channels are based on decompositions of isome-

tries, which are straightforward to adapt to the nearest neighbour case [14, 16].

esting channels. In other words, there are circuits of lower cost than those given in this paper if the channel has a simple or special form. Nevertheless, our constructions could still be used as a starting point to find a low-cost circuit in such cases. Further optimizations could then be performed with algorithms such as, for example, the one given in [8].

For certain special cases, the theory of decomposing operations is quite developed. Considerable effort has been made to reduce the number of C-NOT gates required in the QCM for general unitary gates [9–14] and state preparation [13, 15], which are both examples of a wider class of operations, isometries. Recently, it was shown that every isometry from m to n qubits can be implemented by using about twice the C-NOT count required by a lower bound [16]. This leads to a method to implement quantum channels by using Stinespring’s theorem [17], which states that every quantum channel from m to n qubits can be implemented by an isometry from m to $m+2n$ qubits, followed by tracing out $m+n$ qubits. The isometry can be decomposed into single-qubit gates and 4^{m+n} C-NOTs to leading order [16]. Working in the quantum circuit model this C-NOT count is optimal up to a factor of about four to leading order [16]. However, one can significantly lower this C-NOT count and the required number of ancillas in more general models.

Quantum operations beyond isometries have been investigated in [18]. Although [18] did not focus on a decomposition into elementary gates, combining the decomposition in [18] with an idea given in [19] and with the circuits for isometries given in [16], leads to low-cost decompositions of quantum channels into single-qubit and C-NOT gates in the MeasuredQCM using only one ancilla qubit. The combination of [18] and [19] was fleshed out in [20], which appeared shortly after the first version of the present work. In [20], several applications are also discussed.

In this work, we give a new decomposition and proof that also leads to near-optimal circuits for quantum channels. In contrast to the work mentioned above, we consider channels that map between spaces with different dimensions. Our decomposition can be used for arbitrary channels from m to n qubits (if $m = 0$ our channels allow the preparation of arbitrary mixed states). In spite of the different proof technique, the form of decomposition has similarities with the one based on [18], which we discuss later.

Previously, the task of minimizing the number of required C-NOT gates for the implementation of quantum channels in the MeasuredQCM has been studied in the case of channels on a single qubit [21]. In the special case of a single-qubit channel, we recover a circuit topology (consisting of only one C-NOT gate) similar to that given in [21]. We also note that Ansätze for decompositions of arbitrary channels have been considered in [22, 23]. One of these, Ansatz 1 in [23], is based on applying the Cosine-Sine decomposition to the Stinespring dilation isometry of the channel, and hence will always

work [16]. Our results imply that the Ansatz given in [22] (which is designed for the RandomQCM) cannot work in general because it does not have enough parameters.² Further Ansätze are given in [23], but it is not proven whether these work. In contrast, our constructive decompositions are proven to always work.

In the following we describe how to construct circuit topologies for quantum channels in the two aforementioned generalizations of the quantum circuit model. Our asymptotic results are summarized in Table I. First, we show that in the QCM with additional classical randomness (for free) the number of required ancillas can be reduced to m and the C-NOT count to 2^{2m+n} to leading order. Moreover, we derive a lower bound in this model, which shows that m ancillas are necessary and that our C-NOT count is optimal up to a factor of about two to leading order.

Second, we show that the MeasuredQCM offers further improvement. Our main result is a decomposition scheme for arbitrary m to n channels, which leads to the lowest known C-NOT count of $m \cdot 2^{2m+1} + 2^{m+n}$ if $m < n$ and of $n \cdot 2^{2m+1}$ if $m \geq n$ (to leading order). Moreover, our construction shows that we can implement m to $n \leq m$ channels using only $m+1$ qubits (i.e., one ancilla), and m to $n > m$ channels using n qubits (which is clearly minimal, because the output of the channel is an n -qubit state).

Our construction also leads to low-cost implementations of m to n channels for small m and n (as does the construction resulting from the combination of [18], [19] and [16]). We give the explicit MeasuredQCM topologies for m to n channels for $1 \leq m, n \leq 2$ in Appendix A. These circuits are most likely to be of practical relevance for experiments performed in the near future. In particular, they show that every one to two channel can be implemented with 4 C-NOT gates, every two to one channel with 7 and every two to two channel with 13. These counts are lower than those achieved by working in the QCM or the RandomQCM. For example, the best known implementation of a two to two channel in the quantum circuit model requires about 580 C-NOTs.³ Allowing classical randomness reduces this count to 54 C-NOTs,⁴ which is over four times our C-NOT count of 13 when measurement and classical control are also allowed.

In future work, it would be interesting to generalize our circuit constructions for other universal gate sets. This could be achieved by finding circuits for isometries

² Note that some of the phrasing in [22] gives the impression that this Ansatz is proven to work in all cases; however the authors confirmed that this is not intended.

³ This is an upper bound based on the Column-by-Column Decomposition for isometries [16].

⁴ This corresponds to the C-NOT count for a two to four isometry [16].

TABLE I: Asymptotic upper and lower bounds on the number of C-NOT gates for m to n channels in the three different models (Model 1: QCM, Model 2: RandomQCM, and Model 3: MeasuredQCM). The total number of qubits required for the constructions is also indicated.

Model	Lower bound	Upper bound	Qubits
1 [16]	$\frac{1}{4}4^{m+n}$	4^{m+n}	$m + 2n$
2	$\frac{1}{2}2^{2m+n}$	2^{2m+n}	$m + n$
3 ($m < n$)	$\frac{1}{6}(2^{m+n+1} - 2^{2m})$	$m \cdot 2^{2m+1} + 2^{m+n}$	n
3 ($m \geq n$)	$\frac{1}{6}2^{2n}$	$n \cdot 2^{2m+1}$	$m + 1$

and then applying our construction for channels in the MeasuredQCM described in Section III A, which works independently of the chosen gate set. The ultimate goal would be to design an algorithm that takes as input a given set of gates, a noise model, an accuracy tolerance and a desired operation, and that gives as output a circuit composed of gates from the set that would approximate the desired operation to within the accuracy tolerance (if this is possible), with the number of gates in the circuit being close to minimal. Note that the constructions introduced in this paper could be used as a subroutine in a version of this algorithm, and could serve as a starting point to which further optimizations (to remove gates where possible) are applied.

II. DECOMPOSITION ALLOWING CLASSICAL RANDOMNESS

In the following, we consider the implementation of quantum channels in the RandomQCM, i.e., we allow classical randomness for free. Since the set of all quantum channels from m to n qubits is convex, every m to n channel \mathcal{E} can be decomposed into a (finite) convex combination of extreme m to n channels \mathcal{E}_j .⁵

Physically this means that, allowing classical randomness, the channel $\mathcal{E} = \sum_{j=1}^J p_j \mathcal{E}_j$ can be implemented by performing the channel \mathcal{E}_j with probability p_j (and forgetting about the outcome j).

A. Upper bound

By Remark 6 of [7],⁶ every extreme channel from m to n qubits has Kraus rank at most 2^m . Stinespring's

theorem [17] then implies that in order to implement every extreme channel it suffices to be able to implement arbitrary isometries from m to $m + n$ qubits. Decompositions of such isometries use 2^{2m+n} C-NOT gates to leading order [16]. In the following section, we derive a lower bound on the number of C-NOT gates and ancilla qubits required for m to n channels allowing classical randomness, which shows that the C-NOT count stated above is optimal up to a factor of two in leading order and optimal in the number of required ancillas.

B. Lower bound

Because extreme channels cannot be decomposed into a convex combination of other channels, classical randomness cannot help implement them. Hence, a lower bound for extreme channels in the QCM is also a lower bound for channels in the RandomQCM. Since the set of extreme channels of Kraus rank 2^m is nonempty [24], at least m ancillas are required (using fewer ancillas, we could only generate channels of smaller Kraus rank).⁷ To find a lower bound on the number of C-NOT gates required for a quantum circuit topology for m to n extreme channels, we can use a parameter counting argument, similar to the argument used to derive a lower bound for unitaries [5, 6] or for channels in the quantum circuit model [16].

First, we count the number of (real) parameters required to describe the set of all extreme channels.⁸ Every quantum channel \mathcal{E} from m to n qubits with Kraus rank K can be represented by Kraus operators $A_i \in \text{Mat}_{\mathbb{C}}(2^n \times 2^m)$ such that $\sum_{i=1}^K A_i^\dagger A_i = I$ and $\mathcal{E}(X) = \sum_{i=1}^K A_i X A_i^\dagger$ [for all $X \in \text{Mat}_{\mathbb{C}}(2^m \times 2^m)$] [7]. By Theorem 5 of [7],⁶ a channel \mathcal{E} is extreme if and only if all elements of the set $\{A_i^\dagger A_j\}_{i,j \in \{1,2,\dots,K\}}$ are linearly independent. Each m to n channel \mathcal{E} of Kraus rank $K = 2^m$ can be described by K $2^n \times 2^m$ (complex) matrices A_i , which satisfy 4^m independent (note that the matrix $\sum_{i=1}^K A_i^\dagger A_i$ is Hermitian) conditions (over \mathbb{R}). However, the Kraus representation is not unique. Two sets of Kraus operators $\{A_i\}_{i \in \{1,2,\dots,K\}}$ and $\{B_i\}_{i \in \{1,2,\dots,K\}}$ describe the same channel if and only if there exists a unitary $U \in U(2^m)$, such that $A_i = \sum_{j=1}^K (U)_{i,j} B_j$ [7]. Since a $2^m \times 2^m$ unitary matrix is described by 4^m parameters, we conclude that the set of all extreme channels from m to n qubits is described by $2^{2m+n+1} - 2^{2m+1}$ parameters. Note that the condition that the elements in

⁵ For a bound on the number of channels required see [26].

⁶ In particular, Theorem 5 (and Remark 6) of [7] characterizes the extreme points of the set of all completely positive, unital maps. But the theorem (and the remark) can be adapted to trace preserving (completely positive) maps by considering the adjoint map (see [24] or [26] for more details).

⁷ By a similar argument, one can see that the implementation of channels in the quantum circuit model requires $m + n$ qubits.

⁸ A rigorous mathematical approach of the parameter counting (using the dimension of a differentiable manifold) can be found in [26] and confirms the naive count described here. Note that a parameter count derived within the framework of semi-algebraic geometry was first given in [24].

$\{A_i^\dagger A_j\}_{i,j \in \{1,2,\dots,K\}}$ must be linearly independent is an open condition for $K = 2^m$ and can therefore be ignored for the parameter counting.

A quantum circuit topology for extreme m to n channels must therefore introduce at least $2^{2m+n+1} - 2^{2m+1}$ parameters. Since C-NOT gates cannot introduce parameters into a circuit topology, all the parameters have to be introduced by the single-qubit gates. We work with the following single-qubit rotation gates

$$R_x(\theta) = \begin{pmatrix} \cos[\theta/2] & -i \sin[\theta/2] \\ -i \sin[\theta/2] & \cos[\theta/2] \end{pmatrix}; \quad (1)$$

$$R_y(\theta) = \begin{pmatrix} \cos[\theta/2] & -\sin[\theta/2] \\ \sin[\theta/2] & \cos[\theta/2] \end{pmatrix}; \quad (2)$$

$$R_z(\theta) = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}. \quad (3)$$

For every unitary operation $U \in U(2)$ acting on a single qubit, there exist real numbers α, β, γ and δ such that

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta). \quad (4)$$

A proof of this decomposition can be found in [25]. Note that (by symmetry) equation (4) holds for any two orthogonal rotation axes. The statement above can be represented as a circuit equivalence as follows.

$$-\boxed{U}- = -\boxed{R_z}-\boxed{R_y}-\boxed{R_z}-$$

The wire represents a qubit and the time flows from left to right. We ignore the global phase shift, because it is physically undetectable.

Let us consider l qubits, $l - m$ of which start in a fixed (not necessarily product) state. We can act with a single-qubit gate on each qubit at the beginning of the quantum circuit topology (introducing $3l$ parameters). To introduce further (independent) parameters, we have to introduce C-NOT gates. Naively, one would expect that every C-NOT gate can introduce six new parameters by introducing a single-qubit gate after the control and one after the action-part of it. But by the following commutation relation:

$$\begin{array}{c} \boxed{R_z} \boxed{R_y} \boxed{R_z} \bullet \\ \boxed{R_x} \boxed{R_y} \boxed{R_x} \oplus \end{array} = \begin{array}{c} \boxed{R_z} \boxed{R_y} \bullet \boxed{R_z} \\ \boxed{R_x} \boxed{R_y} \oplus \boxed{R_x} \end{array}$$

each C-NOT gate can introduce at most four parameters. Since we trace out $l - n$ qubits at the end of the circuit, the single-qubit gates on these qubits can not introduce any parameters into the circuit topology [which removes $3(l - n)$ parameters]. We conclude that by using r C-NOT gates we can introduce at most $4r + 3n$ parameters into the circuit topology. By the parameter count above, we require $4r + 3n \geq 2^{2m+n+1} - 2^{2m+1}$ or equivalently $r \geq 2^{2m-1} (2^n - 1) - \frac{3}{4}n$ for a quantum circuit topology that is able to perform arbitrary extreme channels from m to n qubits.

Remark 1 (Lower bound for nonexact circuits)
The derived lower bound can be strengthened and made more general (see [26]): the set of all quantum circuit topologies that have fewer than $\lceil 2^{2m-1} (2^n - 1) - \frac{3}{4}n \rceil$ C-NOT gates, together,⁹ are not able to approximate every m to n extreme channel arbitrarily well. In fact, they can only generate a closed set of measure zero¹⁰ in the smooth manifold of m to n extreme channels of Kraus rank 2^m . Therefore, the lower bound holds for almost every m to n extreme channel of Kraus rank 2^m individually.

III. DECOMPOSITION ALLOWING MEASUREMENT AND CLASSICAL CONTROL

We now move to the consideration of quantum circuit topologies in the MeasuredQCM where we allow measurements (of single qubits in the computational basis) and classical control on the measurement results (and an arbitrary number of ancillas). This generalizes the model used above, since classical randomness can be generated by preparing ancilla qubits in a certain state (by acting with single-qubit unitaries on them), performing measurements and then controlling the parameters of a circuit topology on the measurement results. In the following section we describe how to construct circuit topologies for arbitrary m to n channels of Kraus rank K . Applying this to extreme channels (which have Kraus rank at most 2^m) leads to the C-NOT counts given in Table I. A similar result could be found by using the decomposition described in [18] using binary search [19].

A. Upper bound

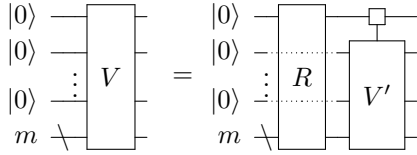
Let \mathcal{E} be a channel from m to n qubits with Kraus rank $K = 2^k$ and Kraus operators $\{A_i\}_{i \in \{1,2,\dots,K\}}$, $A_i \in \text{Mat}_{\mathbb{C}}(2^n \times 2^m)$. We define the matrix $V = [A_1; A_2; \dots; A_K] \in \text{Mat}_{\mathbb{C}}(2^{n+k} \times 2^m)$, by stacking the Kraus operators.¹¹ Since $V^\dagger V = \sum_{i=1}^K A_i^\dagger A_i = I$, we can consider the matrix V as an isometry from m to $n + k$ qubits (which corresponds to a Stinespring dilation of the channel \mathcal{E}). If $n + k = m$ or $k = 0$, we can perform \mathcal{E} by implementing V and tracing out k qubits afterwards. In

⁹ By combinatorial arguments, there are only finitely many different quantum circuit topologies consisting of a fixed number of C-NOT gates (w.l.o.g. we can consider circuit topologies in which we perform single-qubit gates on all qubits at the start of the circuit and two after each C-NOT gate).

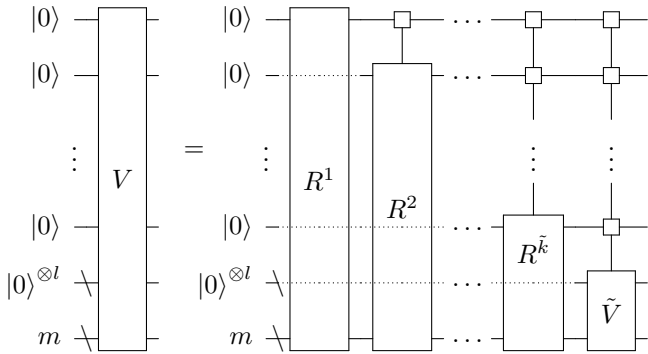
¹⁰ Nevertheless, many interesting operations lie in this set. This is similar to the case of isometries, where, for example, the operation required to implement Shor's algorithm [27] lies in (the analog of) this set [16].

¹¹ For example, we have $[A_1; A_2] := \begin{pmatrix} A_1 \\ A_2 \end{pmatrix}$.

all other cases,¹² we consider each half of the matrix V separately and define $B_0 = [A_1; A_2; \dots; A_{K/2}]$ and $B_1 = [A_{K/2+1}; A_{K/2+2}; \dots; A_K]$. By the QR-Decomposition (for rectangular matrices), we can find unitary matrices $Q_0, Q_1 \in U(2^{n+k-1})$ and $R_0, R_1 \in \{[T; 0; \dots; 0] \in \text{Mat}_{\mathbb{C}}(2^{n+k-1} \times 2^m) : T \in \text{Mat}_{\mathbb{C}}(2^m \times 2^m) \text{ is upper triangular}\}$, such that $Q_0 R_0 = B_0$ and $Q_1 R_1 = B_1$. Note that Q_0 and Q_1 are not unique: indeed only the first 2^m columns are determined and the others are free (up to orthonormality). We can therefore consider Q_0 and Q_1 as isometries from m to $n+k-1$ qubits. Summarized, we have $(Q_0 \oplus Q_1)[R_0; R_1] = V$ and hence, $R := [R_0; R_1] = (Q_0 \oplus Q_1)^\dagger V$ is an isometry. We can represent this decomposition as an equivalence of circuit topologies on $n+k$ qubits, where the first $n+k-m$ start in the state $|0\rangle$ via

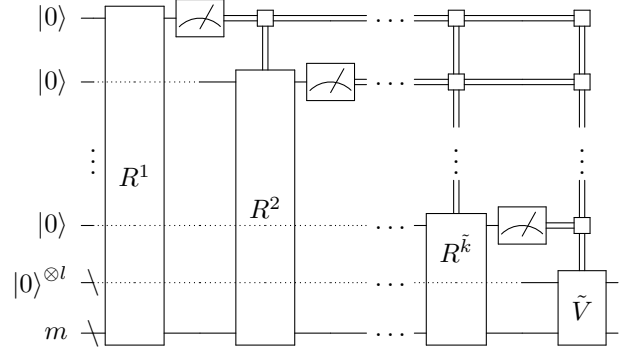


where the backslash stands for a data bus of several (in this case m) qubits and $V' = \{Q_0, Q_1\}$ is a placeholder for two isometries in $\text{Mat}_{\mathbb{C}}(2^{n+k-1} \times 2^m)$. The unfilled square denotes a uniform control.¹³ In the case above, we implement Q_0 if the most significant qubit is in the state $|0\rangle$ and Q_1 if it is in the state $|1\rangle$. Note that the gate R only acts nontrivially on the most significant and the m least significant qubits. In particular, the second to $(n+k-m)$ th qubits are still in the state $|0\rangle$ after applying R (the lack of action of a gate on a particular qubit is indicated by use of a dotted line for that qubit). We can apply the same procedure to the isometries Q_0 and Q_1 . We repeat this k times, until we end up with a quantum circuit topology of the form

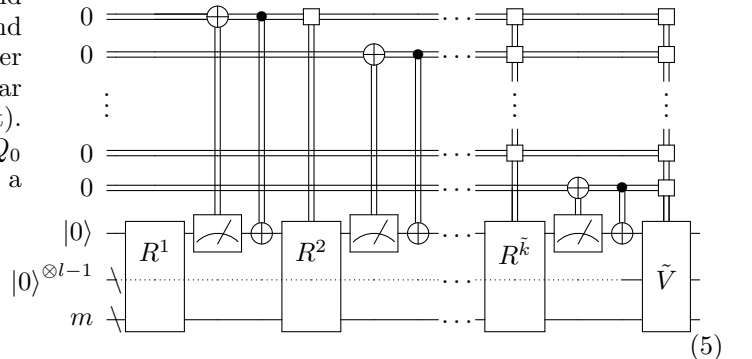


where $\tilde{V} \in \text{Mat}_{\mathbb{C}}(2^{m+l} \times 2^m)$ is an isometry and where each gate R^i acts nontrivially only on the i th and the m

least significant qubits. If $m < n$, we set $l = n - m$ and $\tilde{k} = k$ and if $m \geq n$, we set $l = 1$ and $\tilde{k} = n+k-m-1$. Recall that we can implement the channel \mathcal{E} by applying the isometry V and tracing out the first k qubits afterwards (which we can think about as performing measurements on them and forgetting the result). Since measurements commute with controls, we conclude that the following MeasuredQCM topology is able to perform all channels from m to n qubits of Kraus rank at most K



where we also measure the first $k - \tilde{k}$ of the $l + m$ least significant qubits. Note that the circuit above can be implemented with only one ancilla qubit by resetting it to the state $|0\rangle$ after the measurements and saving the measurement outputs in classical registers



where the second symbol means that a NOT is performed on the first classical register if the output of the first measurement is one.

The construction above can be implemented on a system consisting of $l + m$ qubits. The number of C-NOT gates $N(m, n, k)$ required for the MeasuredQCM topology above is $\tilde{k}N_{\text{Iso}}(m, m+1) + N_{\text{Iso}}(m, m+l)$. Working out the different cases, we conclude that the number of C-NOT gates required for a quantum channel from m to n qubits of Kraus rank 2^k is $N(m, n, k) = N_{\text{Iso}}(m, n)$ if $k = 0$, $N(m, n, k) = N_{\text{Iso}}(m, m)$ if $n + k = m$, and otherwise

$$N(m, n, k) \leq \begin{cases} kN_{\text{Iso}}(m, m+1) + N_{\text{Iso}}(m, n) & \text{if } m < n \\ (k + n - m)N_{\text{Iso}}(m, m+1) & \text{if } m \geq n, \end{cases}$$

where $N_{\text{Iso}}(m, n)$ denotes the number of C-NOT gates required for an m to n isometry. If n is large, we have

¹² Note that for all channels from m to n qubits of Kraus rank $K = 2^k$ we have that $n + k \geq m$ (cf. Lemma 6 of [24]).

¹³ The notation of “uniform control” was introduced in [12]. Some authors also call these gates “multiplexed” (for example, see [14]).

$N_{\text{Iso}}(m, n) \simeq 2^{m+n}$ (for a more precise count, see [16]). Note that the gates R^i are isometries of a special form, which could in principle be implemented by using fewer C-NOTs than an arbitrary isometry. For simplicity, we have not accounted for this in our C-NOT counts. The structure of the gates R^i could be significant when comparing our decomposition to that of [18], which has a similar form to (5) but where the isometries R^i are general (rather than upper triangular).¹⁴

Note that the main idea behind our construction and the requirement of at most one ancilla is general: any decomposition scheme for isometries (including with other universal gate sets; see, e.g., [28]) can be applied to $R^1, R^2, \dots, R^{\tilde{k}}$ and \tilde{V} arising in the decomposition.

B. Lower bound

We expect that allowing measurement and classical controls cannot help when implementing isometries. Since isometries are special cases of channels, we expect further that a MeasuredQCM topology for m to n channels requires $\Omega(2^{m+n})$ C-NOT gates if $m < n$ and $\Omega(4^n)$ C-NOT gates if $m > n$ [16]. Since the proof of this fact is quite technical and uses similar arguments as used to derive the lower bound for extreme channels above, we defer it to Appendix B. The result is summarized in Table I. Note that the lower bound for the case where $m > n$ is quite weak and it would be interesting to improve it in future work.

IV. ACKNOWLEDGEMENTS

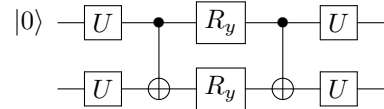
We acknowledge financial support from the European Research Council (ERC Grant Agreement no 337603), the Danish Council for Independent Research (Sapere Aude), the Innovation Fund Denmark via the Qubiz project and VILLUM FONDEN via the QMATH Centre of Excellence (Grant No. 10059). R.C. acknowledges support from the EPSRC's Quantum Communications Hub. The authors are grateful to Bryan Eastin and Steven T. Flammia, whose package Qcircuit.tex was used to produce the circuit diagrams. We thank Jonathan Home for helpful discussions.

Appendix A: Circuits for m to n channels for $1 \leq m, n \leq 2$

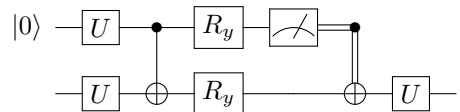
The decomposition scheme in the MeasuredQCM described in Section III A also leads to low-cost circuits for

extreme m to n channels for small m and n . In the following, we demonstrate how to find circuits for m to n channels in the cases where $1 \leq m, n \leq 2$.

1 to 1 channels—An extreme channel from one to one qubit (which is of Kraus rank at most two) can be implemented by performing a one to two isometry followed by tracing out the first qubit. We can use the circuit topology for one to two isometries from Appendix B1 of [16]:

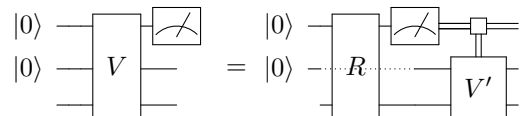


Noting that a unitary before a partial trace can be removed, and that controls commute with measurements, we obtain the following circuit for a one to one channel:



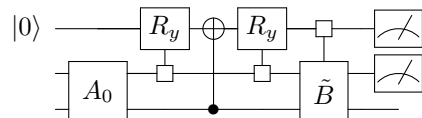
Therefore, any single-qubit channel can be implemented with one C-NOT gate. A similar circuit topology was first derived in [21].

1 to 2 channels—We do the decomposition exactly as described in the general case in Section III A. This leads to a circuit topology of the form



where V is a 1 to 3 isometry corresponding to a Stinespring dilation of the implemented channel and R and V' denote 1 to 2 isometries. We use the circuit topology for one to two isometries given in Appendix B1 of [16] (consisting of two C-NOT gates). Therefore, an extreme channel from one to two qubits (of Kraus rank at most two) requires $2 \cdot N_{\text{Iso}}(1, 2) = 4$ C-NOT gates.

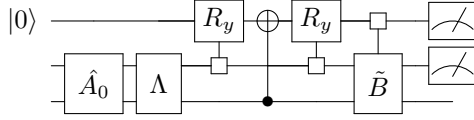
2 to 1 channels—A channel from two qubits to one qubit of Kraus rank at most four can be implemented by an isometry from two to three qubits and tracing out the first two qubits afterwards. We do the first few steps of the decomposition of an two to three isometry as in Appendix B2b of [16]. This leads to the circuit topology



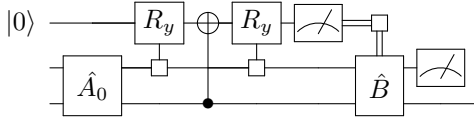
where A_0 and \tilde{B} are two qubit unitaries. We can use a technical trick introduced in Appendix B of [14] to save one C-NOT gate: by Theorem 14 of [14], we can decompose the gate A_0 into a part (which we denote by \hat{A}_0)

¹⁴ On a technical level, the reason for the lack of structure corresponds to the use of the polar decomposition rather than the QR-decomposition.

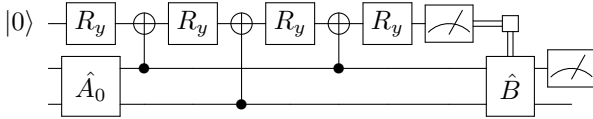
consisting of two C-NOT gates (and single-qubit gates) and a diagonal gate Λ .



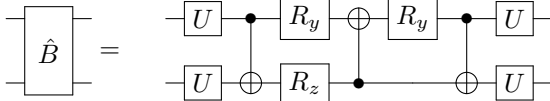
Note that we reversed the gate order of the circuit given in Theorem 14 of [14], such that the diagonal gate is performed after the gate \hat{A}_0 . We commute the diagonal gate Λ to the right and merge it with the gate \hat{B} (and call the merged gate \hat{B}). Therefore, and since controls commute with measurements, the circuit topology given above is equivalent to the following.



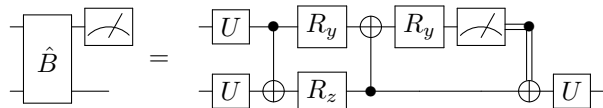
We decompose the uniformly controlled R_y gates as described in Theorem 8 of [14]. Noting that 2 C-NOT gates cancel out each other, we get the following circuit topology.



We can further save one C-NOT gate in the decomposition of the gate \hat{B} . By [5, 6], we have the following equivalence of circuit topologies.



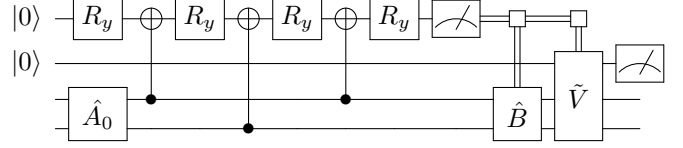
Since controls commute with measurements, we get the following equivalence.



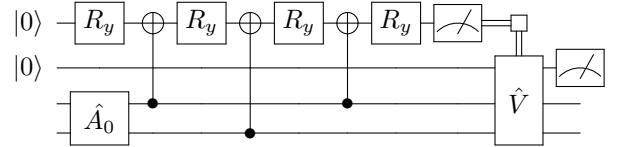
Substituting this circuit into the second-to-last one, we find a circuit topology for channels from two qubits to one qubit of Kraus rank at most four (and hence, in particular, for extreme two to one channels) consisting of 7 C-NOT gates.

2 to 2 channels—This case works similarly to the case of two to one channels of Kraus rank at most four. We use the CSD-approach (cf. [16]) to decompose the isometries arising from the decomposition scheme described in Section III A, and apply the technical tricks introduced in the Appendix of [14]. Indeed, decomposing the first two to three isometry arising in the decomposition described in Section III A as described above in the case of two to

one channels, we find the following circuit for (extreme) two to two channels of Kraus rank at most four



where \tilde{V} denotes the second two to three isometry arising in the decomposition described in Section III A. We can merge the gate \hat{B} into \tilde{V} , which leads to



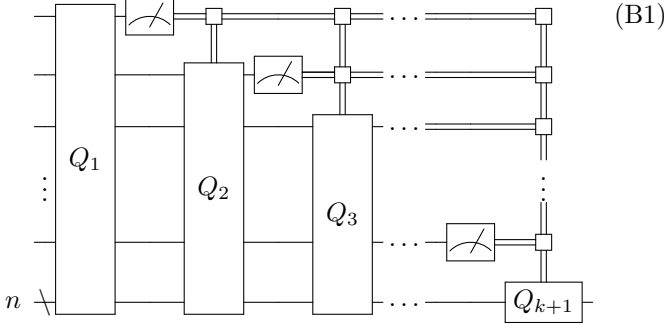
where \hat{V} is a two to three isometry. Therefore, we can again apply the decomposition scheme described above for two to one channels to \hat{V} . Since we do not measure the third qubit at the end of the circuit, we use 8 C-NOT gates to decompose the gate \hat{V} . We conclude that we can decompose any channel from two to two qubits of Kraus rank at most four (and hence, in particular, any extreme two to two channel) with at most 13 C-NOT gates.

Appendix B: Lower bound for isometries in the MeasuredQCM

We give a lower bound on the number of C-NOT gates required for a MeasuredQCM topology that is able to generate all isometries from m to n qubits using the basic gate library comprising arbitrary single-qubit unitaries and C-NOT. A lower bound for m to n isometries in the quantum circuit model was already given in [16]. However, here we work in a more general model than that of [16], since we allow measurements and classical controls (and an arbitrary number of ancillas, each of which start in the state $|0\rangle$).

Let us consider an arbitrary MeasuredQCM topology for m to n isometries consisting of $p \geq n$ qubits. The most general sequence of operations that can be performed by such a circuit topology, is as follows. We perform a certain gate sequence on the p qubits, before the first qubit is measured. Then we perform a second gate sequence on $p-1$ qubits, which may be controlled on the measurement result of the first qubit. Then we measure the second qubit. In the case where we want to measure the first and second qubit together, the second gate sequence can be chosen to be trivial. We go on like this until we have measured $p-n$ qubits. We then forget about the measurement results at the end of the MeasuredQCM topology. Note that the reuse of a qubit after a measurement can be incorporated into the above procedure by adding an additional ancilla qubit and copying the measurement outcome there. We conclude that any

MeasuredQCM topology for m to n isometries consisting of $p \geq n$ qubits can be represented in the following form



where $k := p - n$ and we can think of Q_i as the set of $(p + 1 - i)$ -qubit unitaries that can be generated by the corresponding quantum circuit topology. In other words, there is a first quantum circuit topology (perhaps with free parameters), followed by a measurement, then a classically controlled quantum circuit topology conditioned on the outcome, followed by a second measurement and so on.

Theorem 1 (Lower bound in the MeasuredQCM)

A MeasuredQCM topology that is able to generate all isometries from m to $n \geq m$ qubits using ancillas initialized in the state $|0\rangle$ has to consist of at least $\lceil \frac{1}{6} (2^{n+m+1} - 2^{2m} - \max(2, 3m) - 1) \rceil$ C-NOT gates.

Remark 2 The lower bound given in Theorem 1 is by a constant factor of $\frac{2}{3}$ (to leading order) lower than the one for isometries in the quantum circuit model of $\lceil \frac{1}{4} (2^{n+m+1} - 2^{2m} - 2n - m - 1) \rceil$ C-NOT gates [16]. Intuitively, the use of ancillas, measurements and classical controls should not be helpful for implementing isometries. Therefore, we expect that the lower bound given in Theorem 1 can be improved.

Since isometries from m to n qubits are special cases of m to $n \geq m$ channels, we get the following Corollary.

Corollary 2 A MeasuredQCM topology that is able to generate all channels from m to $n \geq m$ qubits has to consist of at least $\lceil \frac{1}{6} (2^{n+m+1} - 2^{2m} - \max(2, 3m) - 1) \rceil$ C-NOT gates.

Moreover, we find the following lower bound for m to $n < m$ channels.

Corollary 3 A MeasuredQCM topology that is able to generate all channels from m to $n < m$ qubits has to consist of at least $\lceil \frac{1}{6} (4^n - 3n - 1) \rceil$ C-NOT gates.

Proof. Assume to the contrary that there exists a MeasuredQCM topology consisting of fewer than $\lceil \frac{1}{6} (4^n - 3n - 1) \rceil$ C-NOT gates that is able to generate all channels from m to $n < m$ qubits. Such a topology must, in particular, be able to implement all n -qubit unitaries from the first n input qubits to the n output qubits (independently of the state of the other $m - n$ input qubits).

We can turn this topology into a MeasuredQCM topology for unitaries on n qubits by fixing the state of the last $m - n$ input qubits to $|0\rangle$. But such a topology cannot exist by Theorem 1. ■

Before giving the proof of Theorem 1, we sketch the idea. We start with a circuit topology of the form (B1) consisting of $p \geq n$ qubits, $p - m$ of which are initially in the state $|0\rangle$, and assume that it is able to generate all isometries from m to n qubits. In principle, one would expect that a circuit topology controlled on one (randomized) classical bit can introduce twice as many parameters as the circuit topology itself, and hence that controlling on measurement results can help to reduce the C-NOT count (as we saw in Section III A). However, in the special case where we want to implement isometries, the classical control cannot increase the number of introduced parameters. The reason for this is related to the fact that the distribution of the measurement outputs are independent of the input state of the isometry. The precise statement is given in the following Lemma.

Lemma 4 (Independence of measurement results)

Assume that the whole circuit in (B1) performs an isometry from m to n qubits for a certain choice of the free parameters of the MeasuredQCM topology. Then the distribution of the measurement outcomes is independent of the input state of the isometry.

Proof. It suffices to show this for all non-orthogonal states.¹⁵ Take two non-orthogonal input states $|\psi_0\rangle$ and $|\psi_1\rangle$ and assume to the contrary that there exists a measurement M in (B1), whose output distribution is different depending on which of these states is input. Let P be the distribution over the outcomes for M if we choose the input state $|\psi_0\rangle$, and Q be the analogous probability distribution if we choose the input state $|\psi_1\rangle$. Since we are implementing an isometry, the output states $|\psi'_0\rangle := V|\psi_0\rangle$ and $|\psi'_1\rangle := V|\psi_1\rangle$ can be turned back into $|\psi_0\rangle$ and $|\psi_1\rangle$. If we repeat this procedure t times, then, the distribution of outcomes for M is either the i.i.d. distribution $P^{\times t}$ or the i.i.d. distribution $Q^{\times t}$. Since $Q \neq P$ by assumption, these two distributions can be distinguished arbitrarily well for large enough t . This contradicts the fact that in any measurement procedure the maximum probability of correctly guessing which of these states is given as an input is $\frac{1}{2} [1 + D(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|)] < 1$, where D is the trace distance. ■

To handle the independence of the measurement distributions on the input state, it is useful to introduce the concept of postselection (see also [29]). We introduce the Postselected Quantum Circuit Model (PostQCM for

¹⁵ If all non-orthogonal states have the same distribution, then all states do, since the distribution for two orthogonal states $|\psi_0\rangle$ and $|\psi_1\rangle$ must then agree with that of any third state $|\psi\rangle$ that is not orthogonal with both.

short) as a modification of the QCM to include also single-qubit projectors onto the states $|0\rangle$ and $|1\rangle$ at the end of the circuit.¹⁶ Note that the single-qubit projectors correspond to linear maps that are not unitary. We say that a PostQCM topology with associated total linear map C implements the isometry V , if $C = cV$, where $c \neq 0$ is some complex number.

We say that a PostQCM topology corresponds to a MeasuredQCM topology of the form (B1), if it can be obtained from (B1) using the following procedure. First, every measurement is replaced by a single-qubit projector (onto either $|0\rangle$ or $|1\rangle$). Then all classical controls are removed. Finally we move the single-qubit projectors to the end of the circuit. Note that the number of single-qubit gates and C-NOTs of a circuit topology of the form (B1) is the same as that of the PostQCM topology formed by making these replacements.

Lemma 5 *The set of isometries that can be generated by a MeasuredQCM topology of the form (B1) is a subset of the set of isometries that can be generated by all the corresponding PostQCM topologies together.*

Proof. Assume that an isometry V can be generated by a MeasuredQCM topology of the form (B1) for a certain choice of its free parameters. Hence, by Lemma 4, the distribution of the measurement outputs is independent of the input state of the isometry. Therefore, the circuit must perform the isometry regardless of the measurement outputs and hence we can choose and fix an arbitrary output which occurs with nonzero probability. In other words, we can replace each measurement in (B1) with a single-qubit projector onto $|0\rangle$ if the probability of measuring 0 is nonzero, and with a single-qubit projector onto $|1\rangle$ otherwise. Note that this circuit can still perform the isometry V . Removing the classical controls, which does not change the action performed by the whole circuit, we obtain a corresponding PostQCM topology that is able to generate V . ■

Lemma 6 *A PostQCM topology that has fewer than $2^{n+m+1} - 2^{2m} - 1$ free parameters can only generate a set of measure zero of the set of all m to n isometries (where we identify isometries that only differ by a global phase).*

Proof. The argument works similarly to the arguments used in [5, 6, 26]. Let us denote by C the linear map corresponding to the PostQCM topology. We can think of this map as sending a certain choice of d real parameters $(\theta_1, \dots, \theta_d)$ of the PostQCM topology to the corresponding $2^n \times 2^m$ matrix $C(\theta_1, \dots, \theta_d)$, which describes the whole action of the circuit. We restrict the

domain of the free parameters to the set $D \subset \mathbb{R}^d$, such that for all $(\theta_1, \dots, \theta_d) \in D$ there exists an isometry V and a complex number $c \neq 0$, such that $C(\theta_1, \dots, \theta_d) = cV$. We denote the set of one dimensional unitaries by $U(1)$ and define the orbit space $V_{m,n}/U(1)$, which corresponds to the set of all m to n isometries, after quotienting out the (physically undetectable) global phase. We denote the corresponding (smooth) quotient map by $\pi : V_{m,n} \mapsto V_{m,n}/U(1)$ (see [26] for more details). Then, we define the smooth map $T(\theta_1, \dots, \theta_d) := \pi \circ \frac{C(\theta_1, \dots, \theta_d)}{\sqrt{2^{-m} \text{tr } C(\theta_1, \dots, \theta_d)^\dagger C(\theta_1, \dots, \theta_d)}} : D \mapsto V_{m,n}/U(1)$. By Sard's theorem, $T(D)$ is of measure zero in $V_{m,n}/U(1)$ if $d < \dim(V_{m,n}/U(1)) = 2^{m+n+1} - 2^{2m} - 1$. ■

Lemma 7 *A PostQCM topology that consists of fewer than $\lceil \frac{1}{6} (2^{n+m+1} - 2^{2m} - \max(2, 3m) - 1) \rceil$ C-NOT gates (and an arbitrary number of ancilla qubits initialized in the state $|0\rangle$) can only generate a set of measure zero of the set of all m to n isometries.*

Proof. We may assume $n > 1$ (for $n = 1$ the statement of the Lemma is trivial). By Lemma 6, we have left to show that a PostQCM topology consisting of fewer than $\lceil \frac{1}{6} (2^{n+m+1} - 2^{2m} - \max(2, 3m) - 1) \rceil$ C-NOTs cannot introduce $2^{m+n+1} - 2^{2m} - 1$ or more (independent) real parameters. Since single-qubit projections do not introduce parameters into the circuit, all parameters must be introduced by single-qubit gates. To relate the number of single-qubit rotations to the number of C-NOT gates, we use similar arguments to those used in Section II B to derive the lower bound for channels allowing classical randomness. We again use the commutation properties of C-NOT gates and single-qubit rotations, which show that a C-NOT can introduce at most four parameters. However, in contrast to Section II B, we commute all single-qubit rotations to the left (instead of to the right) and use the fact that the first single-qubit rotation on an ancilla can introduce at most two parameters (because an ancilla qubit always starts in the state $|0\rangle$ and two parameters are enough to describe an arbitrary single-qubit pure state). Note that, in general, the single-qubit rotations performed directly before a single-qubit projection have a nontrivial effect on the operation performed by the whole circuit. Thus, a PostQCM topology with q C-NOT gates and consisting of $p \geq n$ qubits can introduce at most $4q + 2(p - m) + 3m$ parameters. Note that we may assume $q \geq \min(p - m, p - 1)$, since otherwise, there exists a collection of ancilla qubits and output qubits (which are not input qubits) that are not quantum-connected to the m input qubits.¹⁷ Any unconnected output qubits that are not input qubits start in the state $|0\rangle$ and al-

¹⁶ Note that this is equivalent to a measurement in the $\{|0\rangle, |1\rangle\}$ basis and postselecting on one of the outcomes.

¹⁷ This follows from a simple statement in graph theory, that a connected graph must have at least $V - 1$ edges, where V denotes the number of vertices of the graph.

ways remain product with the other output qubits.¹⁸ For $n > 1$, the set of isometries for which the output state always has a product form has fewer parameters than the set of arbitrary isometries, and is hence of measure zero. In the case that all the unconnected qubits are ancilla qubits, they have a trivial effect on the performed circuit and can be removed without affecting the action of the circuit. Therefore, a PostQCM topology with q C-NOT gates can introduce at most $6q + \max(2, 3m)$ parameters and hence, a circuit topology consisting of fewer than $\lceil \frac{1}{6} (2^{n+m+1} - 2^{2m} - \max(2, 3m) - 1) \rceil$ C-NOTs cannot introduce $2^{m+n+1} - 2^{2m} - 1$ (or more) parameters. ■

Proof of Theorem 1. Consider a MeasuredQCM topology of the form (B1) consisting of fewer than $\lceil \frac{1}{6} (2^{n+m+1} - 2^{2m} - \max(2, 3m) - 1) \rceil$ C-NOT gates. Since each of the corresponding PostQCM topologies consists of the same number of C-NOT gates, each can only generate a set of measure zero in the set of all m to n isometries by Lemma 7. Since the MeasuredQCM topology (B1) has at most 2^k corresponding PostQCM topologies, the set of isometries that can be generated by all corresponding PostQCM topologies together is still of measure zero. The theorem then follows from Lemma 5 and the fact that a subset of a set of measure zero is again of measure zero. ■

-
- [1] J. T. Barreiro *et al.*, Nature (London) **470**, 486 (2011).
 - [2] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).
 - [3] C. J. Ballance, T. P. Harty, N. M. Linke, M. A. Sepiol, and D. M. Lucas, Phys. Rev. Lett. **117**, 060504 (2016).
 - [4] J. P. Gaebler *et al.*, Phys. Rev. Lett. **117**, 060505 (2016).
 - [5] V. V. Shende, I. L. Markov, and S. S. Bullock, Phys. Rev. A **69**, 062321 (2004).
 - [6] V. Shende, I. Markov, and S. Bullock, in *Proceedings of the Design, Automation and Test in Europe Conference and Exhibition*, Paris, France (IEEE, 2004), p. 980.
 - [7] M.-D. Choi, Lin. Alg. Appl. **10**, 285 (1975).
 - [8] D. Maslov, G. W. Dueck, D. M. Miller, and C. Negrevergne, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems **27**(3), 436, (2008).
 - [9] E. Knill, LANL report LAUR-95-2225, arXiv:quant-ph/9508006 (1995).
 - [10] A. V. Aho and K. M. Svore, quant-ph/0311008 (2003).
 - [11] J. J. Vartiainen, M. Möttönen, and M. M. Salomaa, Phys. Rev. Lett. **92**, 177902 (2004).
 - [12] M. Möttönen, J. J. Vartiainen, V. Bergholm, and M. M. Salomaa, Phys. Rev. Lett. **93**, 130502 (2004).
 - [13] V. Bergholm, J. J. Vartiainen, M. Möttönen, and M. M. Salomaa, Phys. Rev. A **71**, 052330 (2005).
 - [14] V. V. Shende, S. S. Bullock, and I. L. Markov, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems **25**, 1000 (2006).
 - [15] M. Plesch and Č. Brukner, Phys. Rev. A **83**, 032302 (2011).
 - [16] R. Iten, R. Colbeck, I. Kukuljan, J. Home and M. Christandl, Phys. Rev. A **93**, 032318 (2016).
 - [17] W. F. Stinespring, Proc. Amer. Math. Soc. **6**, 211 (1955).
 - [18] S. Lloyd and L. Viola, Phys. Rev. A **65**, 010101(R) (2001).
 - [19] E. Andersson and D. K. L. Oi, Phys. Rev. A **77**, 052104 (2008).
 - [20] C. Shen *et al.*, Phys. Rev. B **95**, 134501 (2017).
 - [21] D.-S. Wang, D. W. Berry, M. C. de Oliveira and B. C. Sanders, Phys. Rev. Lett. **111**, 130504 (2013).
 - [22] D.-S. Wang and B. C. Sanders, New J. Phys. **17**, 043004 (2015).
 - [23] D.-S. Wang, Int. J. Quantum Inform. **14**, 1650045 (2016).
 - [24] S. Friedland and R. Loewy, On the extreme points of quantum channels, arXiv:1309.5898 (2013).
 - [25] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, New York, 2011).
 - [26] R. Iten and R. Colbeck, Smooth Manifold Structure for Extreme Channels, arXiv:1610.02513 (2016).
 - [27] P. Shor, SIAM Journal on Computing **26**, 1484 (1997).
 - [28] E. A. Martinez, T. Monz, D. Nigg, P. Schindler and R. Blatt, New J. Phys. **18**, 063029 (2016).
 - [29] S. Aaronson, in *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences* **461**, p. 3473 (2005).